JUNE 28 - 30, 2005 NORFOLK CONVENTION CENTER

Computer Network Defense (CND)

CDR Dan Currie, USN

Deputy Division Head

PEO C4I & Space/PMW 160.4

29 June 2005

Communications and Networking Session

Sponsored by
SPAWARSYSCOM
FORCEnet Chief Engineer

CND Objectives

- Enterprise CND uniformity
  - Eliminate vulnerabilities caused by legacy network “weak links”
- Information Assurance Protection to Navy
  - Fleet Users Pier side and Deployed
  - OCONUS Users Ashore
- Active Systems to Preempt Unauthorized Activity
  - To Protect, Monitor, Analyze, Detect and Respond
- Proactive Protection to Minimize Security Risk
  - To Modify an Assurance Configuration or Condition
- Support Monitoring, Analysis, and Detection Activities
  - To Provide Trend and Pattern Analysis to Support Multiple Disciplines – Network Operations, Intelligence, Counterintelligence, and Criminal Investigation

CND Is Our Weapon Against The Threat

What We Provide Today

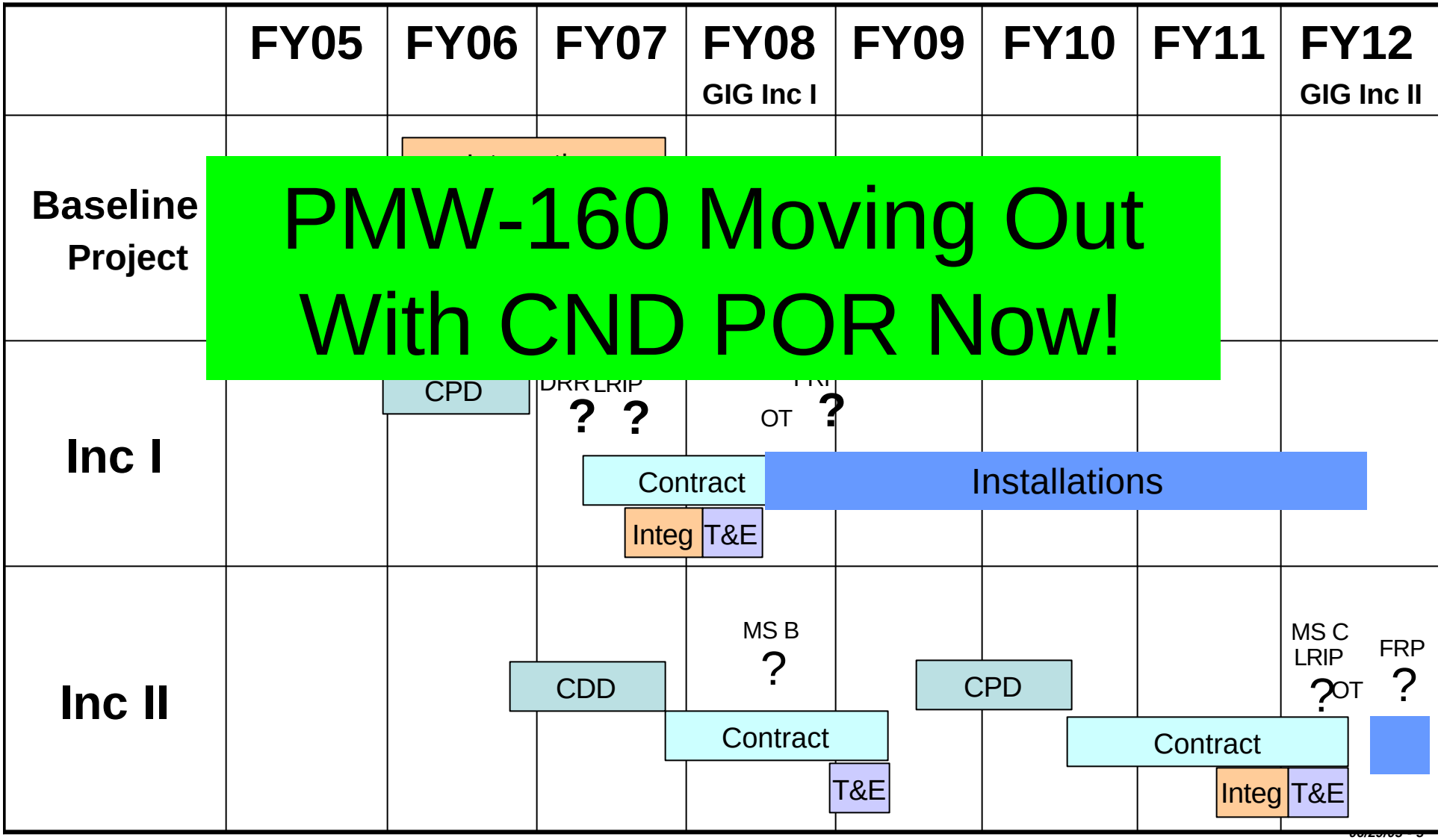
- IA Suites: Firewall, IDS, Antivirus, VPN, Security Screening Routers
- Deployed worldwide and afloat
  - IT21 NOCs
  - ONE-NET Hubs
  - CV, CVN, LHA, LHD, LCC
- Product integration and fielding of joint-developed capabilities (SCCVI, SCRI)
- R&D
- CND Sensor Grid Feeds

Way Ahead:
CND Program of Record

- Computer Network Defense (CND) Baseline
  - CND Provides Virus Protection, Firewalls, Encryption/Decryption, Intrusion Detection for Afloat (IT-21) and
  - Signed by PEO C4I & Space, Dennis Bauman, on 10Nov04
  - Developing Program Strategy and capability documents (CPD, CDD)
  - Identifying additional capabilities to be added to baseline
  - Aligning with GIG IA Capabilities

CND POR will provide uniform application of security for enterprise network

Notional Program of Record Timeline



Focus Areas

- Small Deck CND Solutions
  - Extending CND Services to Unit Level
- Data Correlation & Fusion
  - Focused Information from Large Data Sets
- Automated Responses
  - Intrusion Prevention Systems (IPS) – Rollout in progress
- CND Sensor Grid
  - Security Data Sources from All Nodes
- Automated Vulnerability Management
  - Joint Enterprise Tools (Retina, Hercules)
- Host Based Security
  - INHIBT

Summary – Take Aways

- CND POR will bring uniformity
- Currently fielding initial capabilities
- There is no single solution – a combination of capabilities is required

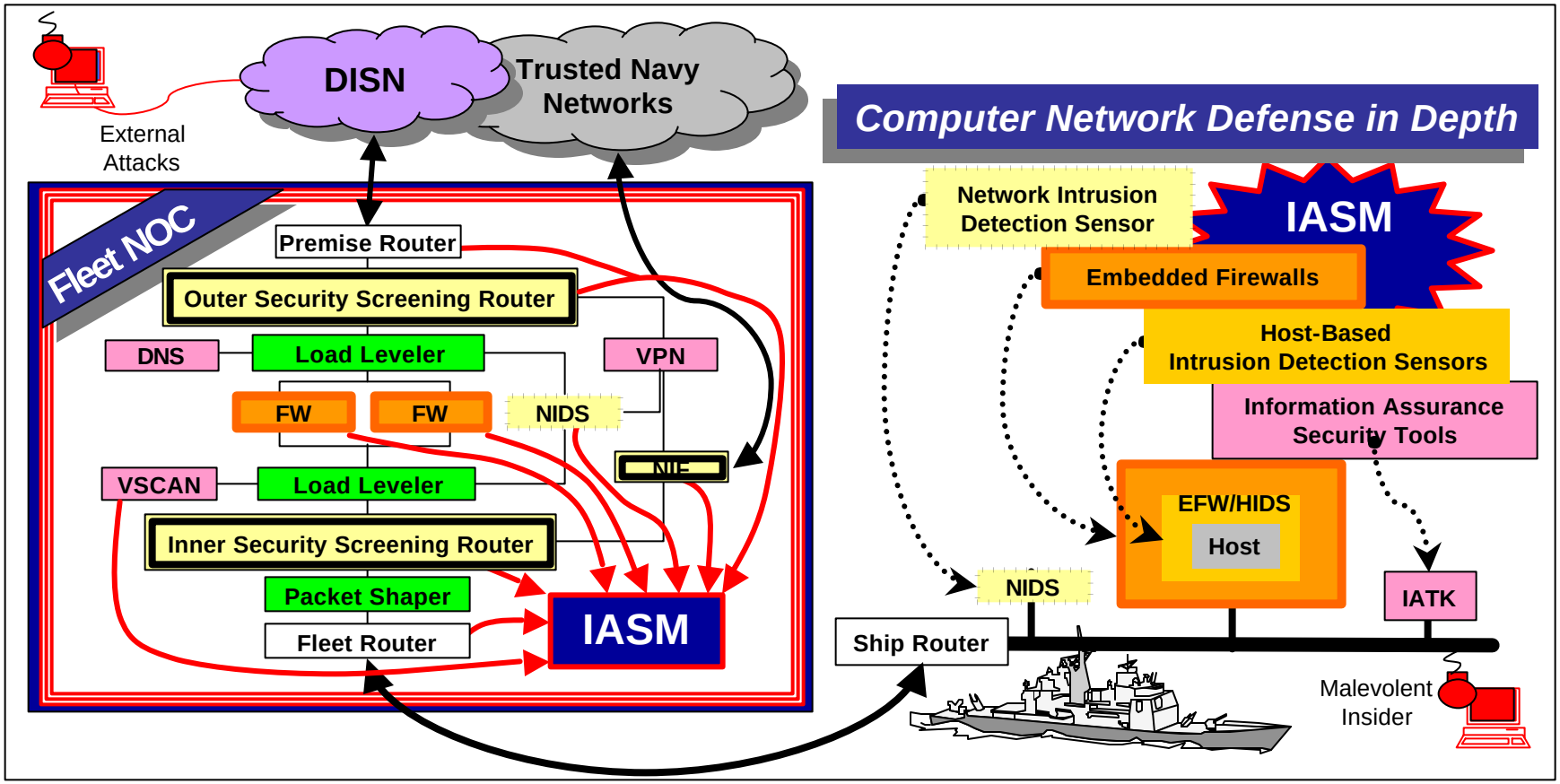
CND Is Our Weapon Against The Threat

Further Info

- Requirements for CND
  - DoDD 8530.1 Computer Network Defense
  - DoDI 8530.2 Support to CND
  - CND ICD (STRATCOM July 2004)
  - GIG IA ICD (NSA – in draft)

Backup

Computer Network Defense (CND)
Shore and Afloat Infrastructure



- Extending the Security Boundaries Beyond the NOC
  - Comprehensive IA Suite at All Fleet NOCs
  - Defense in Depth Strategy at the Afloat Unit Level
  - Protection, Detection, Reaction Capabilities End to End

Navy CND Hierarchy

Tiered Organizational Support Perspective

Network Integration Center

Network Operations Service Centers

Command Control Centers

Norfolk, VA NAVCIRT

Naples, IT Security Operation Center

Yokosuka, JP Security Operation Center

NMCI

ECRNOC

UARNOC

Bahrain Security Operation Center

PRNOC

IORNOC

CONUS

Ship

Ship

Strike Group

Ship

Ship

Bahrain

Naples
Sigonella
Rota
La Maddalena
Souda Bay

Yokosuka
Sasebo
Misawa
Okinawa
Diego Garcia
Singapore

Guam
Atsugi
Korea

CND Sensor Grid

Monitoring for All Environments

Network Integration Center

NAVCIRT
Norfolk, VA

IDS Data

IDS Data

IDS Data

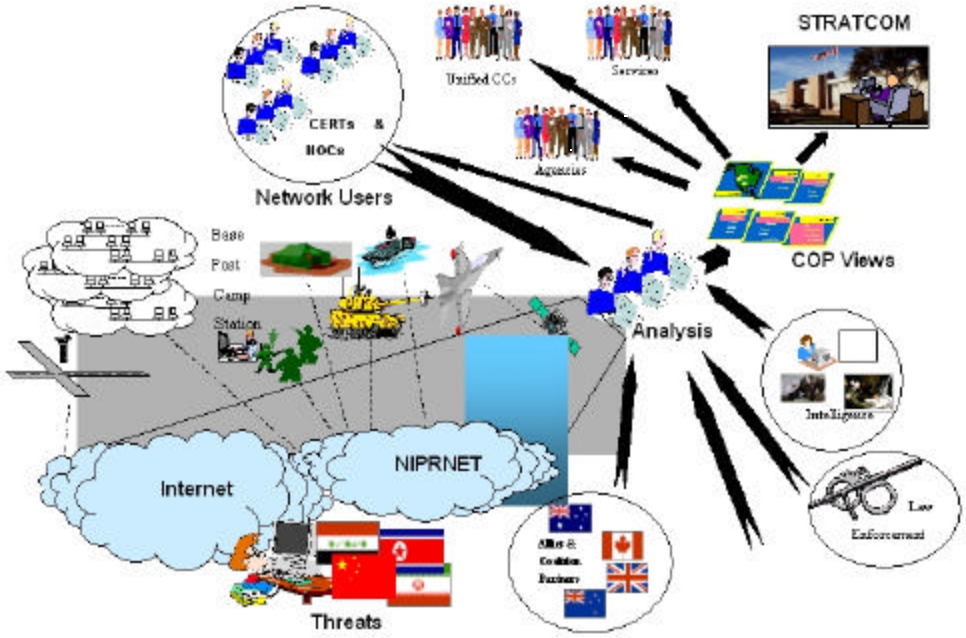
IT21
- UARNOC
- ECRNOC
- IORNOC
- PRNOC

NMCI
- CONUS Sites

ONE-NET
- Naples
- Sigonella
- United Kingdom
- Rota
- La Maddalena
- Souda Bay
- Yokosuka
- Sasebo
- Misawa
- Okinawa
- Diego Garcia
- Singapore
- Guam
- Atsugi
- Korea

Computer Network Defense
Common Operational Picture

- Situational Awareness
  - Builds Shared Picture
  - Common Network Operations
  - Share AS&W Picture and I&W of Threat from all Data Sources
- CND Sensor Grid Based
  - Provides View of Computer Network Activities
    - Monitor Vulnerable Critical Assets
    - Analyze Activity in View of Past Activity
    - Detect & Engage to Control Threat
    - Collect Information to Support AS&W
- Support CND Command & Control Infrastructure
  - Joint Computer Network Operations
  - Navy Component Task Force



CND COP OV-1 Information Exchange Activities
Ref: DoDI O-8530.2